 DBS

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

In the Matter of the Search of Seagate Portable Drive s/n: NA7N87FL located at 775 Ridge Lake Blvd., Ste 300 Memphis, TN	Case No. 23-SW-289

ATTACHMENT C

AFFIDAVIT OF SPECIAL AGENT DANNY SAMPLE

I, DANNY SAMPLE, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKROUND

1. I am a Homeland Security Investigations (HSI) Special Agent (SA) currently assigned to the HSI Memphis Cyber Group. I have been employed with the Homeland Security Investigations since 2018. I am a graduate of the Federal Law Enforcement Training Center in Glynco, Georgia. Before being assigned to HSI Memphis, I was previously assigned to the Internet Crimes against Children (ICAC) group at ASAC Calexico, California. During my tenure with HSI, I have participated in the investigation of cases involving drug offenses, human smuggling, human trafficking, intellectual property rights, firearms offenses, and crimes against children. I have served numerous arrest warrants and participated in the service of search warrants. As part of my duties with the ICAC task force, I investigated criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A, and state law. As part of my training, I have had the opportunity to plan, lead, and participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

2. This affidavit is submitted in support of an application for a search warrant for the portable hard drive described in Attachment A (hereinafter "Target Device"), there being probable cause to believe that located in the Target Device described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A.

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence,

fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A are presently located on the Target Device.

4. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

RELEVANT STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. Sections 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors.

6. 18 U.S.C. Section 2251 prohibits a person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.

7. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B to this Affidavit.

9. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

10. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

11. "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. In this affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical,

electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

SEIZURE AND SEARCH OF STORAGE MEDIA

13. As described above and in Attachment B, I submit there is probable cause to search the Target Device for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. They may be seized and searched on-scene, and/or searched off-scene in a controlled environment.

14. Based upon my training, experience, and consultations with law enforcement officers experienced in child exploitation investigations, and all the facts and opinions set forth in this affidavit, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten.

15. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

16. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how the storage media was used, why it was used, the purpose of its use, and the purposes to which it was put, who used them, the state of mind of the user(s), and when it was used.

17. "User attribution" evidence can also be found on a computer or storage media and is analogous to the search for "indicia of occupancy" while executing a search warrant on the Target Device. For example, registry information, configuration files, user profiles, e-mail,

e-mail address books, "chat," instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the Target Device at a relevant time.

18. Based upon my knowledge, training and experience, I know that a thorough search for information stored in digital storage media requires a variety of techniques that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often agents must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

19. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for permits both on-site seizing, imaging and searching as well as off-site imaging and searching of storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

INVESTIGATION

20. Between April 12, 2023, and April 26, 2023, HSI Special Agent Danny Sample conducted an investigation into the production of child sexual abuse material (CSAM) utilizing the Discord app. Investigators identified as the user of the Discord app that exploited the child as Alan Hayes PAYNE Jr., who resides at 5100 Teal Ave, Memphis (Subject Premises).

21. MPD arrested PAYNE on April 18, for Aggravated Sexual Exploitation of a Minor and PAYNE posted $25,000 bond the following day. Memphis Police Department's (MPD) investigation of PAYNE resulted from a CyberTip received in December 2021. A subsequent search warrant executed on Discord revealed PAYNE uploaded and distributed CSAM and utilized an IP address registered to the Subject Premises.

22. On May 22, 2023, agents with HSI Memphis and investigators assigned to the MPD Internet Crimes Against Children (ICAC) Task Force executed Federal Search Warrant 23-SW-230 on the Subject Premises. Agents knocked and announced their presence and PAYNE's mother, Belinda Payne answered the door, followed shortly thereafter by PAYNE's brother Kris Payne. PAYNE did not arrive at the door until approximately 45 seconds after his brother Kris. As agents knocked and announced their presence, and while encountering PAYNE's mother and brother, ICAC investigator Sgt Paul Hutchison observed someone

throw an object, initially believed to be a cell phone, out of the second story window on the northwest corner of the Subject Premises. The object landed in the back yard of the house located at 5092 Teal Ave., approximately 50 feet from the Subject Premises.

23. After agents cleared the house of potential hazards, SA Sample encountered Sgt Hutchison at the rear of the Subject Premises next to the fence separating the Subject Premises from the back yard of 5092 Teal Ave. Sgt Hutchison told SA Sample that he saw someone throw a cell phone from the upstairs window and that it landed in the back yard of the neighbor's house. To prevent any further damage from either weather, environment, or animals, SA Sample climbed over a waist-high portion of the fence between the two houses and retrieved the object. Upon walking up to the object, SA Sample observed it was a portable hard drive. SA Sample picked up the hard drive using gloves and observed it was a Seagate portable hard drive with a red top case and had dirt stuck to one corner from its impact with the ground. The top portion of the hard drive had a sticker appearing to depict the "Flying Balloon Girl" artwork by graffiti artist Banksy. SA Sample then exited the back yard and placed it in an evidence bag. The window Sgt Hutchison observed the object being thrown from was identified to be PAYNE's room.

24. Based on my training and experience, I know that individuals involved in criminal activity will sometimes attempt to conceal or destroy evidence they believe will be used to incriminate them. Realizing that there is no time to delete incriminating data, individuals attempt to make it appear that a device is not attributable to them because it is not in their immediate control at the time law enforcement conducts a search or encounters an individual. Because the Target Device was observed to be abandoned and thrown out of the window of PAYNE's room, it is probable that the Target Device contains evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 2251, 2252, and 2252A.

25. The Target Device is currently being held by the property custodian in the HSI Memphis evidence vault located at 775 Ridge Lake Blvd., Ste 300, Memphis. Because the Target Device is in the possession of HSI, and HSI agents and analysts may work outside normal business hours, I submit that there is good cause to allow the warrant to be executed at any time of the day or night.

CONCLUSION

26. Based on the investigation described above, probable cause exists to believe that the Target Device contains evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 2251, 2252, and 2252A (described on Attachment B).

27. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

Danny Sample, Special Agent
Homeland Security Investigations

Attested to by the application in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 18th day of July, 2023.

Hon. Tu M. Pham
CHIEF UNITED STATES MAGISTRATE JUDGE